CYLANCE CONSULTING

Merger and Acquisition Security Assessment

Gain Critical Insight into Potential Security Risks

The importance of cybersecurity-related issues throughout the M&A process has increased significantly due to a rise in corporate data breaches and related potential liabilities. Data security issues can lead to large financial losses and can be indicators of risk exposure related to compliance concerns and the organization's reputation in the marketplace.

Cylance Consulting's Merger and Acquisition Security Assessment helps organizations address this uncertainty by allowing M&A participants, including third-party legal firms, to **demonstrate expert due diligence in the determination and preventative reduction of cyber risk**. Armed with information about the security posture of a possible acquisition, companies planning to acquire another can **plan fixes for identified vulnerabilities, use the information to aid decision-making whether to proceed with the acquisition, and may help negotiate a lower purchase price**. The Merger and Acquisition Security Assessment can also be performed after an acquisition is complete but before the IT environments are connected.

Service Overview

Cylance Consulting helps organizations obtain a security baseline of the pending acquisition to reveal the critical information needed to gauge viability and value. Our methodologies leverage artificial intelligence and apply scripts that are quick and lightweight to obtain fast results.

A full Merger and Acquisition Security Assessment is comprised of:

- Compromise Assessment
- External Penetration Test / Vulnerability Assessment
- Internal Penetration Test / Vulnerability Assessment
- Network Architecture Assessment
- NIST Cybersecurity Framework (CSF) Gap Analysis
- Policy Review
- Security Tools Assessment

Compromise Assessment

A Compromise Assessment utilizes a methodology for identifying environmental risks, security incidents, and ongoing threat actor activity in a network environment. The assessment identifies ongoing compromises and uncovers the malicious access and usage of the environment. The goal is to detect and stop any active security incidents quickly and quietly. The assessment addresses core problems such as:

- Data exfiltration and sabotage
- Command and control activities
- User account anomalies

Benefits:

- OS-agnostic assessment across all server and workstation devices on the network without network taps, agents, or monitoring of egress points
- Gain full insight into any potential vulnerabilities on the endpoint, including any previous or actively occurring breaches
- Identify both known and unknown threats across the environment with the goal of moving the environment into a preventative posture from cyber attacks
- Get fast results through methodologies that include artificial intelligence
- Identify shortcomings and resources needed for the security infrastructure to meet industry-recognized best practices

500M

Number of customer records compromised after Marriott's acquisition of Starwood

Source: Forrester, Marriott Breach: Starwood Hacker Gains Access to 500 Million Customer Records

- Malware and persistence mechanisms
- Identification of potential threats and/or vulnerabilities
- Network, host, and application configurations

External Penetration Test / Vulnerability Assessment

The objective of an External Penetration Assessment is to conduct a thorough test of a client's Internet defenses and to identify vulnerabilities that may be difficult or impossible to detect with scanning software. Technical experts use a mix of manual and automated testing techniques in an attempt to gain access to the system and/or sensitive data on the system. Information is collected about the organization's security practices, policies, and procedures to provide recommendations for remediating any vulnerabilities found.

Internal Penetration Test / Vulnerability Assessment

Cylance Consulting's Internal Penetration Assessment begins the internal testing from the perspective of an attacker that has gained a foothold on the internal network. The goal of the assessment is to determine what assets might be exposed to an unauthorized user who has network-level access to a corporate IT environment and help identify the impact of poor access controls as well as mitigate the impact of a malicious or disgruntled employee.

An assessment may include:

- Host discovery
- Footprinting
- Vulnerability scanning
- Manual vulnerability verification
- Penetration testing
- Vulnerability analysis

Network Architecture Assessment

Cylance Consulting's Network Architecture Assessment reviews and identifies any misconfigurations, gaps, weaknesses, and other operational risks in network architecture that could create vulnerabilities. Cylance Consulting security experts will closely inspect an organization's network architecture diagrams, relationships, and solution designs to determine if the rules in place are sufficiently strict, proper network segmentation is in place, and other security configurations are enforced to reduce an organization's attack surface.

NIST Cybersecurity Framework (CSF) Gap Analysis

The goal of Cylance Consulting's NIST CSF Gap Analysis is to evaluate the policies, standards, and procedures implemented by the organization and how they align with the five core functions: identify, protect, detect, respond, and recover. Cylance Consulting's experts will identify positive practices as well as areas for improvement. Elements of consideration include:

- Policy, standards, and procedures
- Program management
- Human resources and organization
- Asset management
- Physical and environmental considerations
- Communications and operations
- Access control
- Information systems management
- Response plans and management
- Regulatory compliance

Policy Review

Cylance Consulting's Policy Review determines the overall state of the client's information security environment and identifies program gaps to improve the overall security posture of the organization. Cylance Consulting will work with the client to identify and provide relevant artifacts around IT and security policies, standards, and procedures, WAN and LAN network diagrams, network data flow diagrams, and vulnerability scan reports that explain how the client identifies, protects, detects, responds, and recovers data and information systems. Cylance Consulting will identify and highlight risks that exist within each security category and provide a gap analysis for each area compared to Cylance Consulting's recommended security baseline.

Security Tools Assessment

Cylance Consulting's Security Tools Assessment evaluates all of the security tools within a client environment to assess redundancy, waste, and poor configuration/implementation. The assessment highlights any gaps in coverage or insufficient capabilities that the organization may have in terms of coverage and implementation.

Deliverables

Cylance Consulting will furnish a comprehensive report detailing:

- Any compromises detected
- A list of vulnerabilities and potential threats
- Detailed anatomy of attacks that were successful during the assessment
- Gap analysis and tool capabilities and functionality
- Strategic and tactical recommendations for remediation
- Assessment findings and alignment of the security policies and procedures to the NIST CSF
- Remediation strategies to achieve compliance with the NIST CSF and industry best practices
- Instructions for developing a roadmap for continuous improvement and monitoring

The reality of the modern business environment is that every organization is vulnerable to cybersecurity problems. It is vital that a full security assessment takes place when considering M&A targets.

Contact Cylance Consulting or your technology provider to discuss your data security needs.

About Cylance Consulting

- World-renowned experts combine subject matter experts from different practice areas to deliver consistent, fast, and effective services around the world
- Incorporates artificial intelligence into tools and back end data analysis processes to more efficiently and effectively secure the environment and *prevent* attacks
- Utilizes multiple techniques to collect information, assess data, provide a risk profile, recommend actions, and highlight notable strengths for an organization
- Techniques are designed to not impact operations in any way
- Integrated practice areas: ThreatZERO™ Services, Incident Containment, and Compromise Assessments, Red Team Services, Industrial Control Systems Security, IoT and Embedded Systems, and Education

+1-877-973-3336
proservices@cylance.com
www.cylance.com/consulting

PS 19-0437-20190619